Haiying Li
Jiangtao Fan

Crime Control of Transnational Telecommunication Network Fraud: Problems and Measures

The global popularization of telecommunication networks has changed the way how citizens communicate in different countries from face-to-face in the limited physical space to virtual space. This has also led to kinds of transnational telecommunication network frauds, that transnational situation in the place of crime behavior, the place of crime result and the place of leasing server. The enhancement of consciousness and ability of criminal's anti-investigation has significantly improved the difficulty of governance. In view of this phenomenon, China has launched special actions to combat this kind of crimes. Although it has made some achievements, the hidden problems have gradually emerged. Therefore, it is necessary to reach a consensus among countries through improving the relevant legislation and signing agreements, to build a mechanism for sharing criminal assets and to control the source of the criminal industrial chain. It can help to reduce the survival space of the crime, which will finally minimize the harm of transnational telecommunications fraud.

Keywords: transnational crimes; telecommunication network fraud; international cooperation; crime control

In recent years, with the advancement of science and technology, telecommunications network technology has become popular all over the world, especially in some remote areas, telecommunications network technology has become a smoother and more convenient way of interpersonal communication. However, science and technology is a double-edged sword. While bringing convenience to people of all countries, it has also been targeted and used by criminals. This has led to the emergence of a new type of crime, telecommunications network fraud, which has greatly affected the development of telecommunications networks. Rickets. Compared with traditional face-to-face scams or limited scams in the region, the telecommunication network has gradually turned from the traditional real space to the virtual cyberspace due to its openness, transnationality and concealment. In turn, it breaks through the embarrassment of traditional time and space, that is, the place of criminal behavior and the result of crime usually spans several countries or regions, and due to some professional technologies of the telecommunication network, it is difficult to collect such crimes, obtain evidence, and arrest Difficulties and law enforcement are difficult. At present, from the perspective of the number of victims and the amount involved, the crime of telecommunication network fraud is becoming more and more serious, and the difficulty of governance is obviously improved, which has brought a strong negative impact and actual harm to the economic and social development of countries in the world, especially developing countries. .

As the world's largest developing country and the world's second largest economy, China's huge economic potential is regarded as a big cake by criminals, and it is a part of the country. Therefore, China has become a high-risk area for the crime of cross-border telecommunication network fraud. . The grim situation of high-profile and frequent scams in cross-border telecommunications networks has attracted the attention of the Chinese government. In June 2015, the State Council approved the establishment of the "Inter-Ministerial Joint Conference on Combating the New Crimes of Telecommunication Network", led by the Ministry of Public Security, and 23 departments and units such as the Ministry of Industry and Information Technology, the Central Propaganda Department, and the People's Bank of China participated in the The fight against telecommunications fraud has become a systematic project to strengthen collaboration and coordinate social resources. This special action has lasted for more than three

years and has achieved remarkable results. For example, the Ministry of Public Security organized 29 public security organs to conduct investigations and investigations abroad, smashed 186 dens, arrested 2,739 criminal suspects, and solved more than 8,000 cases, involving more than 1 billion yuan. In 2017, the public security organs of the country filed a total of more than 30,000 cases of cross-border telecommunication network fraud, down 36.9% year-on-year. Such cases in Beijing, Jiangsu, Zhejiang, Shanghai, Guangdong and other places fell by more than 50%.

The above data shows that China has achieved staged success in tackling cross-border telecommunications network fraud, but in terms of the number of filings, telecommunications network fraud crimes are still at a high level, and with the passage of time, criminals' crime techniques and means become more perfect, the anti-detection ability is gradually enhanced. As a result, the difficulties in governance at this stage have gradually become prominent, which are manifested in the following aspects:

First of all, the relevant legislation of various countries leads to the imbalance of laws due to differences in legislative techniques and national conditions. Because transnational telecommunication networks scam crimes, crime results, server locations, etc. usually involve several countries or regions and even span several continents, the differences between the relevant national laws have created a legal vacuum or loopholes in punishing the crime. It is thus used by criminals to evade the law. For example, the crime of fraud is less severe in Taiwan and Japan, and the Japanese criminal code is usually imprisoned for up to 10 years. In Taiwan, China is usually less than 5 years, but the crime of fraud in mainland China is set as typical. The amount of crimes and plot crimes can be determined to be particularly serious according to the judicial interpretation of 500,000 yuan, and can be sentenced to more than 10 years of imprisonment or even life imprisonment. Therefore, if the crime is committed, some criminals are more willing to accept trials outside the domain. This also indirectly confirms the words of Chen Shiqu, deputy director of the Criminal Investigation Bureau of the former Ministry of Public Security, saying that "the mainland's over 10 million telecom fraud majors are mostly Taiwan's fraud group. For". In the same way, in some developing countries or regions, due to the local economic level, the lag characteristics of Internet and telecommunications legislation and legislative techniques are particularly obvious, which cannot meet the needs of cracking down on international cybercrime, making the original striking force such as The itching is separated and the treatment effect is greatly reduced. Therefore, these places have become a paradise for such criminals.

Secondly, the phenomenon of unsatisfactory international cooperation is outstanding, the procedure for approval of procedures is cumbersome, and the efficiency of collaboration is compromised. With the continuous development of China's economy and technology, domestic technology and other means of technology have advanced by leaps and bounds, and some have even been at the forefront of the world. However, when it was arrested across borders, there were no law enforcement rights and involvement in areas outside mainland China. On the issue of territorial sovereignty, these means of technical investigation are useless. Our judicial personnel mainly rely on the judicial resources provided by the assisting countries to combat the power and discount. In addition, even with the help of the assisting countries, due to the different legal procedures in different countries, when the legal procedures are completed, the opportunity to seize is also missed. Even some fraudulent gangs with strong anti-detection capabilities use the "time of procedure" to transfer positions. In order to avoid the arrest, it may lead to the Chinese investigators failing to return.

Thirdly, the continuous improvement of the strength of multinational fraud organizations has further increased the difficulty of investigating cases. In order to maintain the vitality of their own organizations, multinational fraud groups have also "evolved" their own unique "enterprise" management model. Therefore, gathering "collective wisdom" makes their fraudulent means "evolving" more perfect, especially as a criminal means of high technology. The diversification of

the ways of crime and crime has made the victims of various countries invincible. The longest way for these victims to "walk" is probably the routine of such fraud groups. At the same time, in the process of dealing with the public security organs of various countries for many years, the anti-reconnaissance capabilities of these fraud organizations have gradually increased, and the location of the crimes has been concealed and the modus operandi has become specialized, making the investigation difficult. Moreover, the accumulation of wealth for many years has also enabled the organization's crimes and equipment to be updated one after another, even at the expense of the professional network talents. These have become new challenges for us to detect fraudulent crimes in transnational telecommunications networks.

Finally, the issue of information leakage by Chinese citizens is still frequent, providing convenience for fraudsters to commit crimes. The primary premise of transnational telecommunication network fraud is to illegally obtain citizen's personal information. However, due to the prevention technology and cost, some domestic companies lack comprehensive protection measures for the collected citizen information data, and the protection is weak, even if they are aware of the existence. The problem, however, is still mandatory to collect personal information from customers for commercial purposes. For example, online, when a customer logs in to an account or uses certain service functions, the customer may be forced to enter personal information, otherwise it may not be used normally; or online for commercial considerations or actual needs, often requires real-name registration, such as handling Various membership cards and various kinds of courier are mailed, so the personal information of citizens is very easy to be collected by these enterprises. The number of citizens involved is as few as hundreds of thousands, and the number of citizens is hundreds of millions. The number is extremely impressive and the information content is extremely accurate. high. Therefore, these personal information databases have become the target of criminals. These personal information data are behind a real “naked” citizen whose property has become the criminal object of such criminals. Unfortunately, these personal information databases with huge economic value are acquired by some hackers who have been bought by criminal gangs through technology. Some are directly used by some unscrupulous manufacturers as trading commodities to buy and sell on the “dark net”.

The above difficulties in management are summarized in three aspects, namely, legal issues, technical issues and management issues. For these issues, we propose to solve them through the following channels or methods:

First, implement existing relevant international laws while continuing to improve bilateral or multilateral treaties. Although the United Nations Convention against Transnational Organized Crime, the Cybercrime Convention, and the United Nations Convention against Corruption provide an international legal basis for combating cross-border telecom fraud, these terms usually remain on paper. In reality, we More common is the vacuum of the law and the potential for local protectionism, which has caused obstacles to the arrest of the injured country. Based on the above issues, we believe that we should start from two aspects. On the one hand, we should make the international conventions concrete and operational by improving our domestic laws and further clarifying the legal consensus among countries. On the other hand, we should further clarify the victim countries. The right and the obligation of the assisting country to prevent the injured country from infringing on the sovereignty of other countries on the grounds of pursuing the pursuit of political straits, and also preventing the smuggling of the assisting countries in international cooperation to avoid responsibility, in order to protect the injured country and the victim of the country. The rights of the person.

Second, clarify the position of criminal asset sharing and enhance the enthusiasm of other countries to participate in international judicial cooperation. Article 64 of the Chinese Criminal Law clearly stipulates that “all property obtained by criminals in violation of the law shall be recovered or ordered to be repaid; the legal property of the victim shall be returned in time”, that is, the state

has the right to recover the illegal proceeds of the crime, and the victim Ownership of its legal property, but in the implementation, may be contrary to the fairness provisions, because the assisting country also consumes its own judicial resources in this process, and appropriate and reasonable compensation according to law is reasonable. Therefore, China should clearly define the position of criminal assets sharing in cross-border telecommunication network fraud cases, reasonably share criminal assets, and protect the interests of the country, the assisting country and the victims. Although the "International Criminal Justice Assistance Law of the People's Republic of China (Draft)", which is in the state of brewing, has included the issue of asset sharing, the specific system design is not detailed. In this regard, we believe that on the one hand, it is to clarify the scope and proportion of asset sharing, and at the same time pay attention to the compensation of victims' losses and the protection of the legitimate rights and interests of third parties. On the other hand, it is to establish an alternative to asset sharing and to deal with sharing issues flexibly. This is because we cannot sign a sharing agreement with all countries. Given the tight time, but lack of a sharing basis, giving the assisting country appropriate economic compensation is a good way to promote the recovery of overseas criminal assets.

Finally, pay attention to the problem of source governance of the illegal industrial chain, gradually regulate the management issues of relevant industries and regions involved in the crime of transnational telecommunications network fraud, and compress the living space of such crimes. Although the current cross-border telecommunication network fraud cases cannot be completely eliminated, we can minimize their development. To this end, the primary task is to clean up the living soil of such crimes, that is, to rectify the source of the illegal industrial chain. In reality, the level of economic development varies from country to country, and the legislation is also uneven. Therefore, in the face of such objective conditions, we should actively exert subjective initiative, focusing on criminal hotspots, and aiming at the hotbed and important source of telecommunication network fraud. Place, carry out key control. Since cross-border telecommunication network fraud will inevitably involve capital flow, equipment purchase, information release or communication channels, criminal movement and victim groups, it is necessary to identify and timely identify the above factors through the control of the above factors. Intervene to prevent the emergence of criminal outcomes. This has also put forward new requirements for countries around the world, including China, to carry out standardized management of some key industries and regions in the country, grasping early and grasping small, preventing micro-duration and preventing problems before they occur.

In short, in recent years, cross-border telecommunication network fraud crimes have caused huge economic losses to the countries concerned, including China. Even some cases have affected social stability. Therefore, countries should abandon small profits, focus on the overall situation, and jointly prevent and control it. At the same time, learn from successful experiences and learn lessons, and jointly improve the ability and level of governance of such crimes.